Carnegie Mellon University
Software Engineering Institute

A Mapping of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the Cyber Resilience Review (CRR)

Greg Porter Heinz College, Carnegie Mellon University
Matt Trevors
Robert A. Vrtis

March 2018

TECHNICAL NOTE
CMU/SEI-2018-TN-001

CERT Division
[Distribution Statement A: Approved for Public Release; Distribution is Unlimited]

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM18-0224

Table of Contents

List of Figures

List of Tables

Abstract

This technical note provides a description of the methodology used and observations made while mapping the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the practice questions found in the CERT® Cyber Resilience Review (CRR). The mapping that emerged allows health care and public health organizations to use CRR results not only to gauge their cyber resilience, but to examine their current baseline with respect to the HIPAA Security Rule and the NIST Cybersecurity Framework (CSF). Both the CRR and HIPAA Security Rule have been mapped to the NIST CSF. The authors used these mappings and their extensive experience with CRRs to propose the mapping found in this technical note. The mappings between the CRR practices and the HIPAA Security Rule are intended to be informative and do not imply or guarantee compliance with any laws or regulations. The proposed mapping shows that the CRR provides complete coverage of the HIPAA Security Rule. As a result, organizations that must adhere to the HIPAA Security Rule can use the CRR to indicate their compliance with the Security Rule.

1 Background

1.1 Introduction

The mapping presented in this technical note is proposed by three Senior Engineers who are skilled in the conduct of CERT® Cyber Resilience Reviews (CRRs) and familiar with all practice questions and question guidance. Two members of our team also have several years of experience in the health care and public health sector. Both the CRR and Health Insurance Portability and Accountability Act (HIPAA) Security Rule have each been mapped to the NIST Cybersecurity Framework (CSF) [NIST 2014]. Team members used these mappings and their own experience to propose the mapping found in this technical note. The mappings between the CRR practices and the HIPAA Security Rule are intended to be informative and do not imply or guarantee compliance with any laws or regulations.

The resultant mapping shows that the CRR provides complete coverage of the HIPAA Security Rule. As a result, organizations that must adhere to the HIPAA Security Rule can use the CRR as an indication of their compliance with the Security Rule. Further, about 8% of the CRR questions are not directly applicable to the HIPAA Security Rule, providing insight into an organizations Cyber Resilience beyond the requirements of the Security Rule.

The Department of Health and Human Services Office for Civil Rights published the "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework" in February 2016 for the health care and public health sector to use as an informative reference. These organizations may find the crosswalk helpful as a starting place to identify potential gaps in their programs in assessing their cybersecurity readiness. The Department of Homeland Security (DHS) produced a cyber resilience assessment, the Cyber Resilience Review (CRR) in October, 2011. The CRR is based on Carnegie Mellon University's CERT® Resiliency Management Model (RMM) and is used by DHS in support of Presidential Order 21 to encourage the adoption of the NIST CSF [WH 2013a]. While the CRR predates the establishment of the CSF, the inherent principles and recommended practices within the CRR align closely with the central tenets of the CSF. One should note that both the HIPAA Security Rule and the CRR map well to the CSF.

1.2 What is the HIPAA Security Rule?

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and included a requirement that the Department of Health and Human Services (HHS) draft and promulgate national security standards to ensure appropriate protections for health information that is created, stored, transmitted, or received electronically by covered entities (CEs). The standards, known as the HIPAA Security Rule (the Security Rule), were published on February 20, 2003 to ensure the safeguarding of electronic protected health information (ePHI) managed by covered entities, which include the following:

- Health Care Plans – Any individual or group plan that provides or pays for the cost of medical care (e.g., a health insurance carrier, the Veterans Health Care program, and the Medicare and Medicaid programs).

- Health Care Provider – Any provider of medical or other health services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- Health Care Clearinghouses – A public or private entity that processes health care transactions between covered entities, such as health care plans and providers, from a standard format to a nonstandard format, or vice versa.
- Hybrid Entities – Covered entities that have business activities covered by HIPAA as well as those that are not. Examples include an academic medical center that teaches students (not covered) and also treats patients (covered) or a retailer that sells groceries (not covered) and has on-site pharmacy services to fill prescribed medications (covered).
- Business Associates – The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) expanded the responsibilities of business associates under the HIPAA Security Rule; this important change is further detailed below.

Apart from small health plans that had until April 21, 2006 to comply with the Security Rule, CEs should have been in compliance with the Security Rule no later than April 21, 2005, two years from the original date of publication. However, even today, many covered entities and business associates remain challenged with complying with the requirements of the Security Rule.

The HIPAA Security Rule requires CEs and business associates to maintain reasonable and appropriate administrative, physical, and technical safeguards to protect all individually identifiable health information they manage in electronic form, referred to as ePHI. Specifically, covered entities and business associates must account for the following:

1. ensuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
2. identifying and protecting against reasonably anticipated threats to the security or integrity of the information
3. protecting against reasonably anticipated, impermissible uses or disclosures
4. ensuring compliance by their workforce

With respect to the Security Rule, *confidentialit*y means that only authorized resources such as workforce members may access or disclose ePHI. *Integrity* ensures that ePHI has not been modified or corrupted at rest or in-transit, while *availability* means that authorized workforce members have access to ePHI and supporting technologies, such as an electronic health record (EHR) system, when needed. The HIPAA Security Rule was designed to be flexible, meaning covered entities can exercise their own level of due diligence and due care when selecting security measures that reasonably and appropriately fulfill the intent of the regulations. As a covered entity or business associate evaluates the security measures needed, the organization must consider the following factors:

- the size, complexity, and capabilities of the covered entity or business associate
- the covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities
- the costs of security measures

- the probability and criticality (likelihood of occurrence and business impact) of potential risks to ePHI

The Security Rule is arranged into the following sections and defines them as shown below:

- Administrative Safeguards –"administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." Administrative safeguards are nontechnical measures that govern organizational policy and procedures, workforce member behavior, and appropriate technology usage.
- Physical Safeguards – "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." Physical safeguards pertain to all physical access to ePHI regardless of location (i.e., an on-site facility, the home of a workforce member, or a cloud service provider.)
- Technical Safeguards – "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." Technical safeguards govern information system access and audit controls as well as encryption of ePHI at rest and in transit.
- Organizational Requirements – govern contracts or other arrangements with business associates that covered entities must have in place. Contracts must provide that the business associate will comply with the requirements of the Security Rule and ensure that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the requirements of the Security Rule. Contracts with business associates must also account for how the business associate reports security incidents to the covered entity, including breaches of unsecured protected health information. The standard also includes requirements for a group health plan to ensure that the plan sponsor reasonably and appropriately safeguards ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan.
- Policies and Procedures and Documentation Requirements – require that covered entities and business associates implement reasonable and appropriate policies and procedures to comply with the standards and implementation specifications of the Security Rule, accounting for the maintenance, retention, availability, and updating of such documentation.

The Security Rule contains several security standards with which covered entities and business associates must comply; the standards of the rule are aligned with a series of implementation specifications that provide additional requirements or instructions for fulfilling compliance to a given standard. Implementation specifications are designated as either required or addressable. For required implementation specifications, the organization must comply; however, the exact mechanisms for doing so are at the discretion of the covered entity or business associate, permitting flexibility in terms of how the organization opts to reasonably and appropriately implement the safeguards. Conversely, addressable implementation specifications, while not required, mean that the organization must go through an assessment process by which it analyzes and determines whether a particular implementation specification is reasonable and appropriate with regard to its ability to secure ePHI. In general, after performing the assessment, if the addressable implementation specification is reasonable and appropriate within the context of safeguarding ePHI, then the covered entity or business associate must implement it. However, if the organization deems such implementation is not reasonable and appropriate, then the covered entity or business associate must instead take these steps:

- Document why it would not be reasonable and appropriate to implement the implementation specification.
- Implement an equivalent alternative measure if reasonable and appropriate.

The assessment results and supporting decisions must be documented by the covered entity or business associate. Standards that have no implementation specifications, such as the "Evaluation" and "Audit Controls" standards, are their own implementation specification, and compliance with the standard is required.

Following its issuance, the HIPAA Security Rule remained unchanged until the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009 and amended by the HIPAA Final Omnibus Rule (Omnibus Rule) on January 25, 2013. The Omnibus Rule finalized several provisions of the HIPAA Security Rule that CEs must account for, namely requiring the compliance of business associates (BAs) and their subcontractors with the requirements of the Security Rule. Under the Omnibus Rule, subcontractors of business associates are, by definition, themselves considered business associates if they create, receive, maintain or transmit PHI as a delegated function of the BA. Business associates and subcontractors can be directly liable and subject to criminal and civil liabilities for violations of the HIPAA rules. It is worth noting that the Omnibus Rule modified the definition of "business associate" to include entities that create, receive, maintain, or transmit ePHI for a covered entity. Thus, a vendor persistently storing ePHI over time, such as an outsourced data back-up facility or cloud services provider, on behalf of a covered entity is considered a business associate. Another important aspect of the Omnibus Rule involved the finalization of the HIPAA Breach Notification Rule, requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates via a risk assessment that there is a low probability that the protected health information was compromised. The requisite risk assessment must consider at least the following four factors:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (i.e., whether the information is of a personal sensitive nature such as clinical information or financial details)
2. the unauthorized person who used the PHI or to whom the disclosure was made (i.e., another covered entity that is required to protect the privacy and security of the information or a business or individual who is not required)
3. whether the PHI was actually acquired or viewed
4. the extent to which the risk to the PHI has been mitigated (i.e., obtaining satisfactory assurances from the recipient that the information will not be further used or disclosed)

For breaches affecting 500 or more individuals, covered entities must notify the Secretary of HHS within 60 days of breach discovery. A breach affecting fewer than 500 individuals requires the covered entity to log and report such breaches to the Secretary on an annual basis. A business associate is required to notify the applicable covered entity following breach discovery. The HHS does provide a safe harbor from breach notification requirements for covered entities that render PHI unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or a methodology specified by the Secretary in guidance.

Appendix B of this document provides a crosswalk of the HIPAA Security Rule standards and implementation specifications to the various CRR domains.

1.3 What Is the Cyber Resilience Review (CRR)?

The Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity capabilities [US-CERT 2017a]. The CRR was developed to assist organizations that are part of the critical infrastructure and key resources sectors, as well as organizations that are part of state, local, tribal, and territorial governments.

A CRR assessment is a one-day, interview-based assessment of an organization's cybersecurity management program. It consists of 297 questions about specific cybersecurity practices and is typically delivered in a six-hour workshop led by cybersecurity professionals from the United States Department of Homeland Security (DHS). Using the CRR Self-Assessment package available from DHS, organizations can self-administer the CRR without making use of the cybersecurity experts provided by DHS. The CRR produces a baseline measure of an organization's operational resilience with respect to a specific critical business service and provides a gap analysis for improvement based on recognized best practices.

The CRR allows an organization to baseline its cybersecurity capabilities and maturity to understand its operational resilience. It also allows an organization to manage cyber risk to critical services during normal operations as well as during times of operational stress and crisis. The CRR is based on the CERT® Resilience Management Model (http://www.cert.org/resilience/rmm.html), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience [SEI 2017].

The CERT Division of the SEI developed a crosswalk of the cybersecurity practices measured in the CRR to the criteria of the specific outcomes articulated in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). An organization can use the output of the CRR to approximate its conformance with the NIST CSF. Note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may either fall short of or exceed the corresponding practices and capabilities in the NIST CSF.

1.3.1 CRR Architecture

The CRR comprises 42 goals and 139 specific practices that are extracted from the CERT-RMM and organized into 10 domains:

1. Asset Management

2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

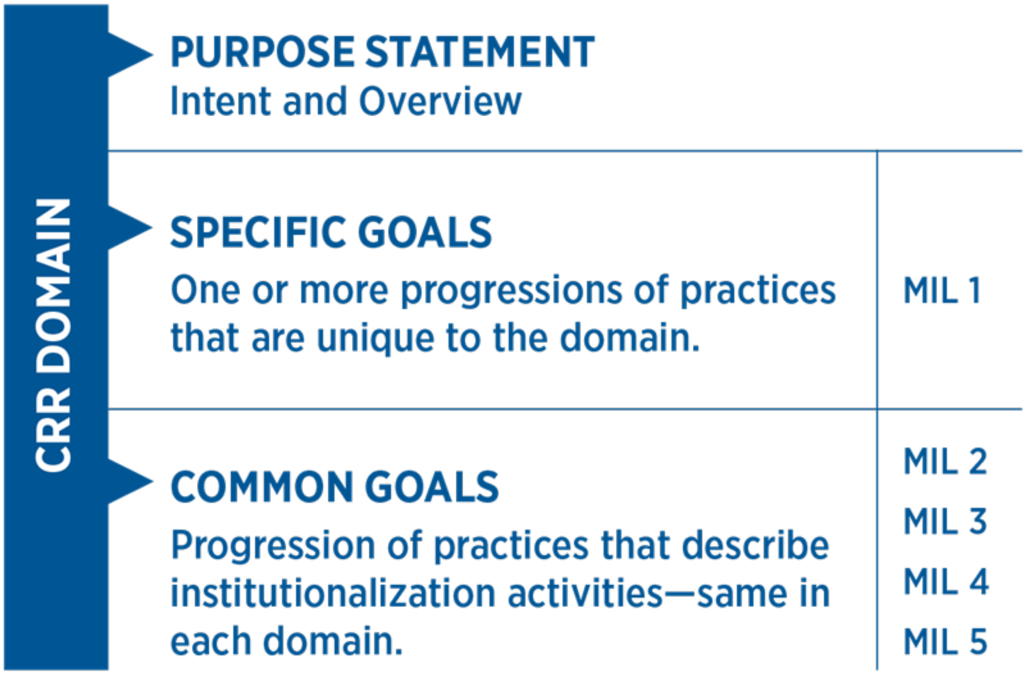
CRR DOMAIN
PURPOSE STATEMENT
Intent and Overview
SPECIFIC GOALS
One or more progressions of practices that are unique to the domain.
MIL 1
COMMON GOALS
Progression of practices that describe institutionalization activities—same in each domain.
MIL 2
MIL 3
MIL 4
MIL 5

Figure 1: CRR Architecture

In this architecture, a core set of goals and practices—referred to as specific goals and practices in CERT-RMM—defines the basic knowledge and skills that must be demonstrated in the domain. The capability maturity dimension is represented by a generic set of goals and practices that indicate increasing levels of capability for performing the core set of goals and practices. Thus, in the CRR, the maturity dimension is singularly measured by the Maturity Indicator Level (MIL) scale. Since the CRR is an assessment and not an audit, it is more appropriate to talk about Maturity Indicators rather than a maturity score.

If an organization performs the practices that would allow it to meet the specific goals for a domain, the organization is said to be achieving the domain in a performed state: the practices that define the domain are observable, but no determination can be made about the degree to which these practices are

- repeatable under varying conditions

- consistently applied
- able to produce predictable and acceptable outcomes
- retained during times of stress

Testing for these conditions requires applying a common set of 13 MIL questions to the domain, but only after MIL1 is achieved.

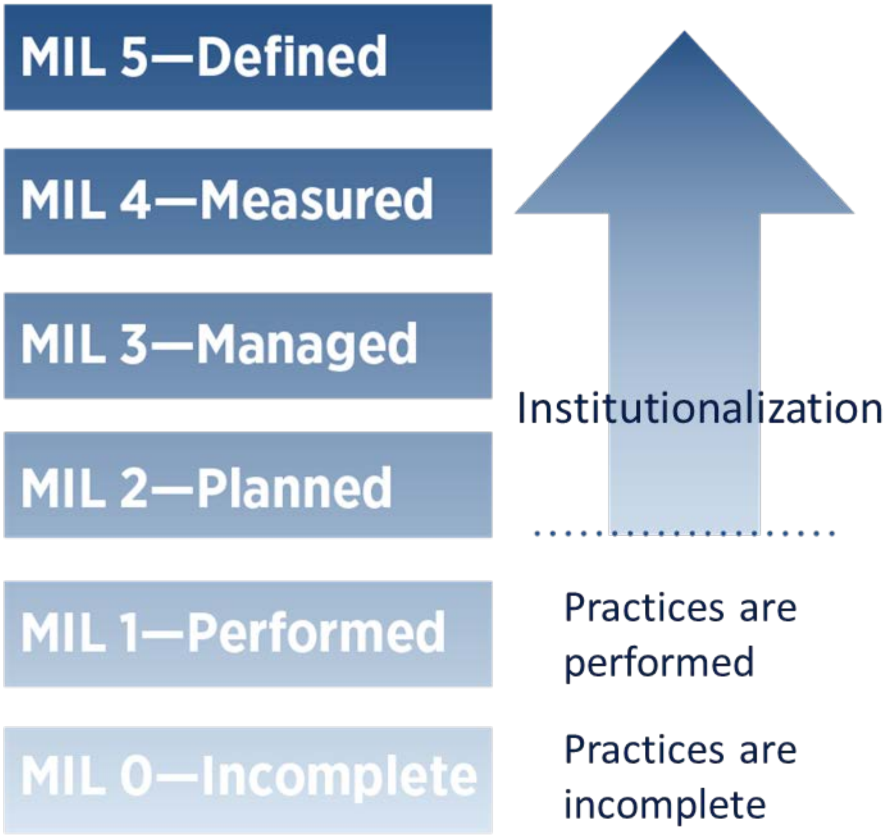

Figure 2: MIL Scale

As shown in the MIL scale, MILs are cumulative; to achieve a MIL in a specific domain, an organization must perform all of the practices in that level and in the preceding MILs. For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain.

1.4 What is the NIST Cybersecurity Framework (CSF)?

The president issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013 to better address cybersecurity risks [WH 2013b]. The Executive Order stated “it is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.” In enacting this policy, the Executive Order calls for the development of a voluntary, risk-based, Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework was created through collaboration between government and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses. The Framework focuses on using business drivers to guide cybersecurity activities.

The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Framework enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today’s multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

The Executive Order also directed sector-specific agencies to “review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments” [WH 2013b].

1.5 What Does This Technical Note Provide?

This technical note provides information necessary to help an organization evaluate the effectiveness of its enterprise cybersecurity program. While covered entities and business associates are required by law to comply with both the HIPAA Privacy Rule and the HIPAA Security Rule, this may not be enough to establish a comprehensive cybersecurity program. The CRR encompasses 10 domains organizing the practices organizations should implement in order to assist with establishing an effective enterprise-wide cybersecurity management program. This technical note provides a section-by-section mapping of the HIPAA Security Rule as it relates to the CRR domains, goals, and specific practices. The mapping can be used to help organizations use the results of a CRR assessment to examine the completeness of their existing policies, plan, processes, and procedures as they relate to the HIPAA Security Rule, the NIST CSF, and the CRR. Using the one-day, lightweight assessment allows an organization to examine its cybersecurity program compliance with the requirements of the HIPAA Security Rule, while highlighting where gaps may exist in implementing a more comprehensive cybersecurity management program that would further improve its resilience to cyber attacks.

The crosswalk in this technical note, along with the recommended additions to CRR question guidance it contains, is meant to assist cybersecurity professionals who administer a CRR. The baseline the organization obtains after participating in the six-hour CRR workshop allows the organization to baseline its cybersecurity capabilities in a context focused on the health care and public health sectors regulatory environment as articulated in the HIPAA Security Rule.

This technical note provides a description of the methodology used to develop the crosswalk of the CRR practices to the HIPAA Security Rule standards and implementation specifications. It was specifically developed with the intent of facilitating the use of the CRR as an indicator of cybersecurity readiness of organizations within the health care and public health sector. Both tools have been independently mapped to the NIST CSF, and this technical note uses those independent mappings to map the CRR and the HIPAA Security Rule.

Other sector specific agencies, such as the financial sector, water sector and electric sector, have developed their own tools; the methodology described here can be used to develop additional mappings in a similar fashion.

2 How to Use this Mapping

As mentioned previously, this mapping represents the relationships between the HIPAA Security Rule and the CRR, an assessment tool used to evaluate an organization’s critical business service across 10 domains. There are multiple ways to use this mapping. The first, and likely most useful, is for an organization to review its cybersecurity program and determine which parts of the program are related to each section of the HIPAA Security Rule administrative, physical, and technical safeguards. From that point, an organization can refer to the mapping to cross-reference CRR questions related to each of the administrative, physical, and technical safeguards. This mapping helps an organization determine not only if its implementation meets the requirements of the HIPAA Security Rule, but if it is also an effective control as defined by the criteria in the related CRR question. If the CRR question is not clear, the user may expand the ⓘ icon on the self-assessment form to reveal information related to the question. The user requiring further guidance on addressing the CRR question can refer to the code or codes at the end of the question. The format of the code resembles the following [XXXX:SGx.SPy]. These codes represent specific practices of the CERT-RMM or Resilience Management Model. An organization can review these practices by downloading the CERT-RMM from the CERT.org website. Alternatively, an organization could conduct a CRR assessment. This can be done either by asking the local Cybersecurity Adviser (CSA) to conduct a facilitated assessment or downloading the CRR Self-Assessment material from the Critical Infrastructure Cyber Community Voluntary Program website [US-CERT 2017b]. In addition to the self-assessment form, the user can also review the CRR Resource Guides that provide detailed information on how to address each of the 10 domains identified in the CRR.

(The organization should also have access to 45 Code of Federal Regulation Parts 164.308, 164.310, and 164.312, otherwise known as the HIPAA Security Rule Administrative, Physical, and Technical Safeguards.)

3 Approach

Although a published mapping between the HIPAA Security Rule and the CRR did not exist prior to this project, mappings for both to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) were available. The mapping of the HIPAA Security Rule to the NIST CSF was developed by the collaboration of NIST and the Department of Health and Human Services, Office of the National Coordinator for Health IT (ONC), and is available on the HHS.gov website https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html [HHS 2016]. CERT, at the request of the Department of Homeland Security, authored and published the mapping between the CRR and the NIST CSF. The mapping of the CRR to the NIST CSF is available at the C3 Voluntary Program website hosted by US-CERT at https://www.us-cert.gov/ccubedvp/self-service-crr [US-CERT 2017c].

As the basis for an initial mapping between HIPAA Security Rule and the CRR, the team chose to accept a common mapping to a NIST CSF subcategory. For example, HIPAA Security Rule Section 164.308(a)(1)(ii)(A) mapped to NIST CSF sub-category ID.AM-2 (function – Identify, category – Asset Management, subcategory 1). CRR practice AM:G1.Q3 (domain –Asset Management, goal 1, question 3) is also mapped to NIST CSF ID.AM-2. The team would initially assume that HIPAA Security Rule Section 164.308(a)(1)(ii)(A) directly mapped to CRR AM: G1.Q3.

With the initial mapping exercise completed, the team began the process of customizing the mapping by conducting the following activities:

- Ensure each initial mapping was applicable and appropriate.
- Propose applicable mappings from the HIPAA security rule to the CRR that had not been identified by the initial crosswalk.
- Propose additional information to be added to the CRR's question guidance that would help the CRR Navigator interpret the CRR practice in the context of a member of the health care sector.

Upon completion of the customization exercise the team was able to complete the following:

- Remove inapplicable or inappropriate mappings (8% reduction).
- Create previously unidentified mappings (15% addition).

The customization exercise showed the CRR providing complete coverage of the HIPAA Security Rule. Moreover, approximately 8% of the CRR Maturity Indicator Level 1 (Performed) questions were not directly applicable to the HIPAA Security Rule.

For example, The CRR's Asset Management domain contains the following practice questions that are not directly addressed by the HIPAA Security Rule:

- Are services identified?
- Are services prioritized based on analysis of the potential impact if the services are disrupted?
- Are asset descriptions updated when changes to assets occur?

The Controls Management domain also contains three practice questions that are not addressed:

- Are control objectives (requirements) prioritized according to their potential to affect the critical service?
- Are control designs analyzed to identify gaps where control objectives are not adequately satisfied?
- As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps?

It may seem that these practices are commonly in place and simply best practices; however, in our experience assessing over 300 organizations across all sectors, what seem to be "best practices" are not uniformly implemented and are not always followed by the majority of the organizations being assessed.

Using the mappings of the CRR and HIPAA Security Rule to the NIST CSF, we propose the mapping of the CRR practices to the HIPPA Security Rule's declarative statements found in Appendix B.

4 Correlation of the HIPAA Security Rule and the CRR

4.1 Description of the Layout of the Mapping

The mapping, listed as Appendix B, is the result of research we conducted for this technical note. The mapping used NIST mapping of the CSF to the HIPAA Security Rule [DHHS 2016] and the CERT mapping of the CRR to the CSF [SEI 2016], as well as real-world industry experience to identify correlations between the HIPAA Security Rule's administrative, physical, and technical safeguards and the cyber resilience review.

The X-Axis of the mapping contains all of the sections from the Code for Federal Regulations Title 45, Sections 164.308, 164.310, and 164.312 or Administrative Safeguards, Physical Safeguards, and Technical Safeguards respectively. The Y-Axis contains a listing of all CRR domains, goals, and their related questions. An X at an intersection means the team identified a strong connection between the text in the HIPAA Security Rule and the CRR practice question. This connection may become evident simply through reading of the text. However, some connections required deeper research that included identifying practices identified in the NIST mapping between the HIPAA Security Rule and the Cybersecurity Framework as well as the Health and Human Services mapping between the HIPAA Security Rule and NIST 800-53 Revision 3.

For example, moving across the X-axis to 164.308(a)(1(ii)(B), which states "Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)" and down the Y-Axis to Vulnerability Management G1:Q1 (Goal 1, question 1), which asks "Has a vulnerability analysis and resolution strategy been developed?" reveals a correlation between the HIPAA Security Rule section and the CRR practice question. By reviewing the CRR question directly, the reader will notice the CERT-RMM specific practice associated with the question. In this instance, that specific practice is VAR:SG1.SP2 – Establish a Vulnerability Analysis and Resolution Strategy. At this point the reader may choose to review the question guidance associated with the CRR question or may choose to review the CERT-RMM specific practice by downloading CERT-RMM from http://www.cert.org/resilience/rmm.html. Reviewing both the question guidance and the CERT-RMM specific practice(s) associated with the questions is encouraged.

5 Conclusions

During the mapping process, it became evident that the CRR provided guidance on each and every section of the HIPAA Security Rule’s administrative, technical, and physical safeguards. This correlation may provide organizations with assurance, or justified confidence, that answering the CRR questions in the affirmative indicates they have implemented the practices necessary to effectively address both the requirements of the HIPAA Security Rule and develop a resilient critical business service. Ultimately, it is up to the organization to ensure its policies, plans, processes, and procedures meet the requirements of the law.

Examining the reverse mapping, using the CRR as a measuring stick, the HIPAA Security Rule’s administrative, physical, and technical safeguards contain gaps in coverage and can be augmented to more thoroughly identify the policies, plans, processes, and procedures necessary to adequately protect the confidentiality, integrity, and availability of electronic protected health information. Reviewing the mapping presented here, a reader can identify that eight out of ten CRR domains contain questions that do not map directly to any section in the HIPAA Security Rule.

Although many of these practices may seem to be best practices that organizations would routinely implement, our experience has shown that organizations do not routinely put “best practices” in place without being motivated to do so by routine assessments and reviews by management. Reviewing the mapping will reveal many more “best practices” that are not addressed by the rule. The HIPAA Security Rule forms a regulatory foundation but it is paramount for health care organizations to expand their review of their cybersecurity management practices to help identify any chinks in their cyber resilience armor.

6 Definitions

addressable implementation specifications – specifications that, while not required, stipulate that the organization go through an assessment process by which they analyze and determine whether a particular implementation specification is reasonable and appropriate with regard to its ability to secure ePHI.

administrative safeguards – the administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information (as defined in the Security Rule).

availability – assurance that only authorized workforce members have access to ePHI and supporting technologies, such as an electronic health record (EHR) system, when needed.

breach – an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

business associates – entities that create, receive, maintain, or transmit ePHI for a covered entity. Thus, a vendor persistently storing ePHI over time, such as an outsourced data back-up facility or cloud services provider, on behalf of a covered entity means that the vendor is a business associate. The Omnibus Rule modified the definition to include these entities.

Under the Omnibus Rule, subcontractors of business associates are, by definition, themselves considered business associates if they create, receive, maintain or transmit PHI as a delegated function of the BA. Business associates and subcontractors can be directly liable and subject to criminal and civil liabilities for violations of the HIPAA rules.

confidentiality – assurance that only authorized resources such as workforce members may access or disclose ePHI.

cyber event – a cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation).

cyber incident – actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

cyber resilience – the ability of a system or domain to withstand cyber attacks or failures, and in such events, to reestablish itself quickly.

integrity – assurance that ePHI has not been modified or corrupted at rest or in transit.

physical safeguards – the physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion (as defined in the Security Rule).

required implementation specifications – the specifications with which organization must comply; however, the exact mechanisms for doing so are at the discretion of the covered entity or business associate, permitting flexibility in terms of how the organization opts to reasonably and appropriately implement the safeguards.

technical safeguards – the technology and the policy and procedures for its use that protect electronic protected health information and control access to it (as defined in the Security Rule).

standards that have no implementation specifications – standards such as the “Evaluation” and “Audit Controls” standards that are their own implementation specification and for which compliance with the standard is required.

Appendix A Executive Order – Improving Critical Infrastructure Cybersecurity

This executive order is accessible at https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the Program).

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Appendix B HIPAA Security Rule > CRR Crosswalk

This appendix contains a proposed mapping between the Cyber Resilience Review and HIPAA Security Rule. This mapping was developed by members of the CERT Division of the Software Engineering Institute and could be used to inform a discussion with the developers of the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework document.

Cyber Resilience Review

The Cyber Resilience Review (CRR) was developed with the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications, as a no-cost, non-technical assessment to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis.

CERT has developed a correlation of the practices measured in the CRR to criteria of the NIST Cybersecurity Framework (CSF). An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of, or exceed, corresponding practices and capabilities in the NIST CSF.

HIPAA Security Rule Crosswalk to the NIST CSF

The following information is taken from the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework document dated February 22, 2016 and found at https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

In the health care space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Privacy Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain, or transmit. The crosswalk document we used identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule.

The mapping was developed to allow organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule a starting place to identify potential gaps in their programs. Addressing these gaps can bolster their compliance with the Security Rule and improve their ability to secure ePHI and other critical information and business processes. For example, if a covered entity has an existing security program aligned to the HIPAA Security Rule, the entity can use this mapping document to identify which pieces of the NIST Cybersecurity Framework it is already meeting and which represent new practices to incorporate into its risk management program. This mapping document also allows organizations to communicate activities and outcomes internally and externally regarding their cybersecurity program by using the Cybersecurity Framework as a common language. Finally, the mapping can be easily combined with similar mappings to account for additional organizational considerations (e.g., privacy, regulation and legislation). Additional resources, including a FAQ and overview, are available to assist organizations with the use and implementation of the NIST Cybersecurity Framework.

This crosswalk maps each administrative, physical, and technical safeguard standard and implementation specification in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework subcategory. Due to the granularity of the NIST Cybersecurity Framework's subcategories, some HIPAA Security Rule requirements may map to more than one subcategory. Activities to be performed for a particular Subcategory of the NIST Cybersecurity Framework may be more specific and detailed than those performed for the mapped HIPAA Security Rule requirement. However, the HIPAA Security Rule is designed to be flexible, scalable and technology-neutral, which enables it to accommodate integration with frameworks such as the NIST Cybersecurity Framework. A HIPAA covered entity or business associate should be able to assess and implement new and evolving technologies and best practices that it determines would be reasonable and appropriate to ensure the confidentiality, integrity, and availability of the ePHI it creates, receives, maintains, or transmits.

The mappings between the Framework subcategories and the HIPAA Security Rule are intended to be an informative reference and do not imply or guarantee compliance with any laws or regulations. Users who have aligned their security program to the NIST Cybersecurity Framework should not assume that by so doing they are in full compliance with the Security Rule. Conversely, the HIPAA Security Rule does not require covered entities to integrate the Cybersecurity Framework into their security management programs. Covered entities and business associates should perform their own security risk analyses to identify and mitigate threats to the ePHI they create, receive, maintain or transmit.

Table 1: Administrative Safeguards (164.308)

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
Asset Management																															
G1:Q1																															0
G1:Q2																															0
G1:Q3																															0
G1:Q4																										X					1
G2:Q1	X										X																				2
G2:Q2																													X		1
G2:Q3																															0
G2:Q4																															0
G2:Q5	X						X			X																X					4
G3:Q1																										X					1
G3:Q2		X									X							X								X					4
G4:Q1																															0
G4:Q2																															0
G5:Q1		X				X		X	X	X		X										X		X							8
G5:Q2						X						X																			2
G5:Q3						X			X	X		X	X				X														6
G5:Q4						X			X	X		X	X																		5

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G5:Q5						X						X	X																		3
G5:Q6						X						X	X			X															4
G6:Q1										X																					1
G6:Q2																															0
G6:Q3																															0
G6:Q4																															0
G6:Q5																						X	X								2
G6:Q6																															0
G6:Q7	X																														1
G7:Q1																															0
G7:Q2																															0
G7:Q3																					X			X							2
Controls Management																															
G1:Q1																															0
G1:Q2																															0
G2:Q1																															0
G2:Q2																															0
G2:Q3												X	X					X													3

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G2:Q4												X	X					X													3
G2:Q5																															0
G2:Q6				X													X														2
G2:Q7						X	X																								2
G2:Q8																															0
G2:Q9			X										X																		2
G2:Q10												X	X																		2
G3:Q1																															0
G3:Q2																															0
G4:Q1																															0
G4:Q2																															0
Configuration and Change Management																															
G1:Q1																											X				1
G1:Q2																															0
G1:Q3	X	X																													2
G1:Q4																															0
G1:Q5																															0
G1:Q6																															0

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G2:Q1																											X				1
G2:Q2				X																											1
G2:Q3																															0
G2:Q4																															0
G2:Q5				X																											1
G2:Q6																															0
G2:Q7																															0
G2:Q8																															0
G2:Q9							X																								1
G2:Q10							X																								1
G2:Q11				X			X										X														3
G3:Q1																							X								1
G3:Q2																															0
G3:Q3				X																											1
G3:Q4				X																											1
G3:Q5				X																											1
G3:Q6				X																											1

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
Vulnerability Management																															
G1:Q1	X	X														X															3
G1:Q2																X											X				2
G1:Q3				X												X															2
G1:Q4				X												X															2
G1:Q5				X												X	X														3
G2:Q1																X															1
G2:Q2																X															1
G2:Q3	X															X															2
G2:Q4																X															1
G2:Q5																X															1
G2:Q6	X															X															2
G3:Q1	X	X														X				X											4
G3:Q2																															0
G3:Q3																X															1
G4:Q1																X															1
Incident Management																															
G1:Q1					X		X	X											X												4

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G1:Q2																			X												1
G1:Q3																															0
G1:Q4					X														X												2
G2:Q1							X									X	X			X											4
G2:Q2																				X											1
G2:Q3																				X											1
G2:Q4				X												X	X			X											4
G2:Q5																				X											1
G2:Q6																				X											1
G2:Q7				X												X				X											3
G2:Q8																				X											1
G2:Q9																			X												1
G3:Q1				X															X												2
G3:Q2							X												X												2
G3:Q3																				X											1
G4:Q1																				X											1
G4:Q2																			X	X											2
G4:Q3																X	X		X	X											4
G4:Q4																				X											1

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G5:Q1																				X											1
G5:Q2																				X											1
G5:Q3																				X											1
Service Continuity Management																															
G1:Q1																					X			X							2
G1:Q2																								X							1
G1:Q3																						X		X							2
G1:Q4																								X							1
G1:Q5																								X							1
G1:Q6																						X	X	X							3
G2:Q1																								X	X	X					3
G3:Q1																									X						1
G3:Q2																															0
G3:Q3																						X	X		X						3
G3:Q4																							X		X						2
G3:Q5																									X	X					2
G4:Q1																						X		X							2
G4:Q2																								X	X						2

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G4:Q3																								X	X						2
Risk Management																															
G1:Q1																															0
G1:Q2																															0
G1:Q3		X																									X				2
G1:Q4																															0
G2:Q1		X																	X												2
G2:Q2																															0
G2:Q3		X																		X	X					X					4
G2:Q4		X																													1
G3:Q1	X	X		X																						X					4
G4:Q1	X	X																								X					3
G4:Q2																											X				1
G5:Q1																															0
G5:Q2																															0
External Dependencies Management																															
G1:Q1									X	X																		X			3
G1:Q2																												X			1

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G1:Q3																												X			1
G2:Q1	X																											X	X	X	4
G3:Q1				X																								X			2
G3:Q2																												X			1
G3:Q3																												X			1
G3:Q4																												X			1
G4:Q1				X																								X			2
G4:Q2																												X			1
G4:Q3																												X			1
G4:Q4																															0
G5:Q1																												X			1
G5:Q2																												X			1
Training and Awareness																															
G1:Q1														X																	1
G1:Q2														X																	1
G1:Q3														X	X																2
G1:Q4														X																	1
G2:Q1														X																	1

CRR/ HIPAA SR	a1iiA	a1iiB	a1ii C	a1iiD	a2	a3i	a3iiA	a3iiB	a3ii C	a4i	a4iiA	a4iiB	a4ii C	a5i	a5iiA	a5iiB	a5ii C	a5iiD	a6i	a6ii	a7i	a7iiA	a7iiB	a7ii C	a7iiD	a7iiE	a8	b1	b2	b3	CRR Ref
G2:Q2														X																	1
G2:Q3														X	X																2
G2:Q4														X	X																2
G2:Q5					X	X								X		X	X	X													6
G2:Q6					X	X								X		X															4
G2:Q7					X	X								X																	3
Situational Awareness																															
G1:Q1																X															1
G1:Q2	X	X		X											X	X															5
G1:Q3																X															1
G2:Q1																				X											1
G2:Q2																				X											1
G3:Q1															X																1
G3:Q2																															0
G3:Q3																															0
Total HIPAA SR	12	12	1	18	5	10	8	2	4	6	2	9	8	11	5	24	8	4	9	20	3	6	5	12	7	9	5	13	2	1	

Table 2: Physical Safeguards (164.310)

CRR/ HIPAA SR	a1	A2i	a2ii	A2iii	a2iv	b	c	d1	d2i	d2ii	d2iii	d2iv	CRR Ref
Asset Management													
G1:Q1													0
G1:Q2													0
G1:Q3													0
G1:Q4													0
G2:Q1						X	X	X	X	X	X		6
G2:Q2		X	X			X	X	X	X	X	X		8
G2:Q3		X				X	X	X	X	X	X		7
G2:Q4		X	X			X	X	X	X	X	X		8
G2:Q5													0
G3:Q1		X											1
G3:Q2	X(F)	X	X				X				X		5
G4:Q1													0
G4:Q2											X		1
G5:Q1	X(F)	X	X	X		X	X	X			X		8
G5:Q2	X(F)	X	X	X			X	X			X		7
G5:Q3	X(F)	X	X	X		X	X						6
G5:Q4	X(F)	X	X	X		X	X						6
G5:Q5	X(F)	X	X	X		X	X						6
G5:Q6	X(F)	X	X	X		X	X						6
G6:Q1							X	X		X	X		4
G6:Q2							X	X		X	X		4
G6:Q3							X	X		X	X		4
G6:Q4							X	X		X	X		4
G6:Q5		X					X	X		X	X	X	6
G6:Q6				X	X		X	X	X	X	X		7
G6:Q7				X	X		X	X	X	X	X		7
G7:Q1		X											1
G7:Q2		X											1
G7:Q3	X	X	X										3

CRR/ HIPAA SR	a1	A2i	a2ii	A2iii	a2iv	b	c	d1	d2i	d2ii	d2iii	d2iv	CRR Ref
Controls Management													
G1:Q1	X(F)					X							2
G1:Q2													0
G2:Q1	X			X									2
G2:Q2			X			X	X						3
G2:Q3			X			X	X	X					4
G2:Q4			X			X	X						3
G2:Q5						X	X	X					3
G2:Q6	X		X	X	X	X	X	X			X		8
G2:Q7			X			X	X	X	X				5
G2:Q8							X						1
G2:Q9							X						1
G2:Q10						X	X						2
G3:Q1													0
G3:Q2													0
G4:Q1	X												1
G4:Q2	X			X		X	X						4
Configuration and Change Management													
G1:Q1	X(F)		X				X						3
G1:Q2	X(F)		X				X						3
G1:Q3												X	1
G1:Q4													0
G1:Q5													0
G1:Q6													0
G2:Q1													0
G2:Q2			X			X							2
G2:Q3			X			X							2
G2:Q4			X	X		X							3
G2:Q5			X										1
G2:Q6			X	X	X	X	X						5
G2:Q7													0

CRR/ HIPAA SR	a1	A2i	a2ii	A2iii	a2iv	b	c	d1	d2i	d2ii	d2iii	d2iv	CRR Ref
G2:Q8			X			X	X						3
G2:Q9			X		X		X	X					4
G2:Q10			X		X		X	X					4
G2:Q11			X	X	X		X	X		X	X		7
G3:Q1						X							1
G3:Q2													0
G3:Q3													0
G3:Q4													0
G3:Q5													0
G3:Q6													0
Vulnerability Management													
G1:Q1	X(F)		X	X			X						4
G1:Q2	X(F)		X	X			X						4
G1:Q3													0
G1:Q4													0
G1:Q5	X		X	X			X	X			X		6
G2:Q1	X(F)			X									2
G2:Q2	X(F)			X									2
G2:Q3	X(F)		X	X				X					4
G2:Q4	X(F)		X	X									3
G2:Q5	X(F)		X	X									3
G2:Q6	X(F)												1
G3:Q1								X					1
G3:Q2													0
G3:Q3													0
G4:Q1													0
Incident Management													
G1:Q1		X		X									2
G1:Q2													0
G1:Q3													0

CRR/ HIPAA SR	a1	A2i	a2ii	A2iii	a2iv	b	c	d1	d2i	d2ii	d2iii	d2iv	CRR Ref
G1:Q4		X		X									2
G2:Q1		X	X	X		X	X	X			X		7
G2:Q2				X		X	X	X			X		5
G2:Q3				X		X	X	X			X		5
G2:Q4				X		X	X	X			X		5
G2:Q5				X		X	X	X			X		5
G2:Q6				X		X	X	X			X		5
G2:Q7				X		X	X	X			X		5
G2:Q8				X		X	X	X			X		5
G2:Q9				X		X	X	X			X		5
G3:Q1													0
G3:Q2													0
G3:Q3													0
G4:Q1		X											1
G4:Q2		X											1
G4:Q3													0
G4:Q4													0
G5:Q1													0
G5:Q2													0
G5:Q3													0
Service Continuity Management													
G1:Q1	X(F)	X											2
G1:Q2		X											1
G1:Q3		X											1
G1:Q4		X											1
G1:Q5		X											1
G1:Q6		X											1
G2:Q1		X											1
G3:Q1													0
G3:Q2													0
G3:Q3		X											1

CRR/ HIPAA SR	a1	A2i	a2ii	A2iii	a2iv	b	c	d1	d2i	d2ii	d2iii	d2iv	CRR Ref
G3:Q4		X										X	2
G3:Q5		X											1
G4:Q1		X											1
G4:Q2		X											1
G4:Q3		X											1
Risk Management													
G1:Q1		X	X										2
G1:Q2													0
G1:Q3		X	X										2
G1:Q4													0
G2:Q1													0
G2:Q2													0
G2:Q3		X	X										2
G2:Q4		X	X										2
G3:Q1		X											1
G4:Q1		X											1
G4:Q2													0
G5:Q1													0
G5:Q2													0
External Dependencies Management													
G1:Q1		X											1
G1:Q2													0
G1:Q3													0
G2:Q1		X											1
G3:Q1		X											1
G3:Q2		X											1
G3:Q3		X											1
G3:Q4		X											1
G4:Q1		X											1
G4:Q2		X											1

CRR/ HIPAA SR	a1	A2i	a2ii	A2iii	a2iv	b	c	d1	d2i	d2ii	d2iii	d2iv	CRR Ref
G4:Q3		X											1
G4:Q4		X											1
G5:Q1		X											1
G5:Q2		X											1
Training and Awareness													
G1:Q1													0
G1:Q2													0
G1:Q3													0
G1:Q4													0
G2:Q1													0
G2:Q2													0
G2:Q3													0
G2:Q4													0
G2:Q5		X				X	X						3
G2:Q6													0
G2:Q7		X	X	X									3
Situational Awareness													
G1:Q1	X(F)												1
G1:Q2	X			X									2
G1:Q3													0
G2:Q1													0
G2:Q2													0
G3:Q1													0
G3:Q2													0
G3:Q3													0
Total References	12	12	1	18	5	10	8	2	4	6	2	9	

Table 3: Technical Safeguards (164.312)

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
Asset Management														
G1:Q1													0	0
G1:Q2													0	0
G1:Q3													0	0
G1:Q4													0	1
G2:Q1					X								1	9
G2:Q2	X		X		X			X					4	13
G2:Q3	X		X		X								3	10
G2:Q4	X		X		X								3	11
G2:Q5					X								1	5
G3:Q1			X										1	3
G3:Q2			X	X	X		X	X	X		X		7	16
G4:Q1													0	0
G4:Q2													0	1
G5:Q1	X	X	X	X			X	X	X		X	X	9	25
G5:Q2	X	X	X	X				X	X			X	7	16
G5:Q3	X	X	X				X	X	X				6	18
G5:Q4	X	X	X					X	X				5	16
G5:Q5	X	X	X				X	X	X				6	15
G5:Q6	X	X	X				X	X	X				6	16
G6:Q1	X				X		X						3	8
G6:Q2	X				X		X						3	7
G6:Q3					X		X						2	6
G6:Q4							X						1	5
G6:Q5			X				X	X					3	11
G6:Q6							X				X		2	9
G6:Q7							X				X		2	10
G7:Q1			X										1	2
G7:Q2			X										1	2
G7:Q3			X										1	6

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
Controls Management														
G1:Q1				X			X						2	4
G1:Q2													0	0
G2:Q1				X			X						2	4
G2:Q2				X			X			X			3	6
G2:Q3		X		X	X	X	X	X	X			X	8	15
G2:Q4		X		X	X	X	X	X		X	X	X	9	15
G2:Q5				X	X	X							3	6
G2:Q6		X		X		X	X						4	14
G2:Q7		X		X	X	X	X					X	6	13
G2:Q8		X			X	X	X	X		X		X	7	8
G2:Q9	X								X				2	5
G2:Q10	X	X		X			X						4	8
G3:Q1													0	0
G3:Q2													0	0
G4:Q1													0	1
G4:Q2													0	4
Configuration and Change Management														
G1:Q1													0	4
G1:Q2													0	3
G1:Q3													0	3
G1:Q4													0	0
G1:Q5													0	0
G1:Q6													0	0
G2:Q1													0	1
G2:Q2						X			X		X		3	6
G2:Q3									X	X			2	4
G2:Q4	X	X				X	X	X	X		X		7	10
G2:Q5	X	X				X	X	X	X	X	X		8	10

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
G2:Q6	X	X				X	X		X				5	10
G2:Q7													0	0
G2:Q8	X			X									2	5
G2:Q9		X											1	6
G2:Q10													0	5
G2:Q11	X	X				X		X			X		5	15
G3:Q1				X									1	3
G3:Q2													0	0
G3:Q3						X							1	2
G3:Q4						X							1	2
G3:Q5	X			X		X							3	4
G3:Q6	X			X		X							3	4
Vulnerability Management														
G1:Q1													0	7
G1:Q2								X		X	X		3	9
G1:Q3								X		X	X		3	5
G1:Q4								X			X		2	4
G1:Q5						X		X		X	X		4	13
G2:Q1													0	3
G2:Q2													0	3
G2:Q3		X				X		X		X			4	10
G2:Q4													0	4
G2:Q5													0	4
G2:Q6		X											1	4
G3:Q1													0	5
G3:Q2													0	0
G3:Q3													0	1
G4:Q1													0	1

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
Incident Management														
G1:Q1		X	X		X								3	9
G1:Q2													0	1
G1:Q3													0	0
G1:Q4			X										1	5
G2:Q1		X				X		X		X	X		5	16
G2:Q2		X			X	X							3	9
G2:Q3													0	6
G2:Q4			X			X							2	11
G2:Q5													0	6
G2:Q6						X							1	7
G2:Q7						X							1	9
G2:Q8					X	X							2	8
G2:Q9													0	6
G3:Q1													0	2
G3:Q2			X										1	3
G3:Q3			X										1	2
G4:Q1			X										1	3
G4:Q2			X										1	4
G4:Q3													0	4
G4:Q4													0	1
G5:Q1													0	1
G5:Q2													0	1
G5:Q3													0	1
Service Continuity Management														
G1:Q1			X										1	5
G1:Q2			X										1	3
G1:Q3			X										1	4
G1:Q4			X										1	3
G1:Q5			X										1	3

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
G1:Q6			X				X						2	6
G2:Q1			X										1	5
G3:Q1													0	1
G3:Q2													0	0
G3:Q3			X										1	5
G3:Q4			X				X						2	6
G3:Q5			X										1	4
G4:Q1			X										1	4
G4:Q2			X										1	4
G4:Q3			X										1	4
Risk Management														
G1:Q1			X										1	3
G1:Q2													0	0
G1:Q3													0	4
G1:Q4													0	0
G2:Q1			X										1	3
G2:Q2													0	0
G2:Q3													0	6
G2:Q4													0	3
G3:Q1			X										1	6
G4:Q1			X										1	5
G4:Q2													0	1
G5:Q1			X										1	1
G5:Q2													0	0
External Dependencies Management														
G1:Q1			X										1	5
G1:Q2													0	1
G1:Q3													0	1
G2:Q1			X										1	6

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
G3:Q1			X										1	4
G3:Q2			X										1	3
G3:Q3			X				X						2	4
G3:Q4			X				X						2	4
G4:Q1													0	3
G4:Q2													0	2
G4:Q3													0	2
G4:Q4													0	1
G5:Q1			X										1	3
G5:Q2			X										1	3
Training and Awareness														
G1:Q1													0	1
G1:Q2													0	1
G1:Q3													0	2
G1:Q4													0	1
G2:Q1													0	1
G2:Q2													0	1
G2:Q3													0	2
G2:Q4													0	2
G2:Q5							X		X				2	11
G2:Q6													0	4
G2:Q7							X		X				2	8
Situational Awareness														
G1:Q1													0	2
G1:Q2		X				X	X	X					4	11
G1:Q3						X	X						2	3
G2:Q1													0	1
G2:Q2													0	1
G3:Q1													0	1

CRR/ HIPAA SR	a1	a2i	a2ii	a2iii	a2iv	b	c1	c2	d	e1	e2i	e2ii	CRR Ref	Total CRR Ref
G3:Q2													0	0
G3:Q3													0	0
Total References		23	48	16	17	25	32	22	16	10	14	6		

References

URLs are valid as of the publication date of this document.

[DHHS 2016]
DHHS Office for Civil Rights. HIPAA Security Crosswalk to NIST Cybersecurity Framework. 2016. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

[HHS 2016]
Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between IPAA Security Rule and NIST Cybersecurity Framework. *HHS.gov*. 2016. https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

[NIST 2014]
National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.* 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf p6

[SEI 2016]
Software Engineering Institute CERT Division, Carnegie Mellon University. Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks. 2016. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf

[SEI 2017]
The CERT Resilience Management Model (CERT-RMM). Software Engineering Institute, Carnegie Mellon University. February 15, 2018 [accessed] http://www.cert.org/resilience/rmm.html

[US-CERT 2017a]
Current Activity. *US-CERT*. February 15, 2018 [accessed]. https://www.us-cert.gov/

[US-CERT 2017b]
Critical Infrastructure Cyber Community Voluntary Program. *US-CERT*. February 15, 2018 [accessed]. https://www.us-cert.gov/ccubedvp

[US-CERT 2017c]
Assessment: Cyber Resilience Review (CRR). *US-CERT*. February 15, 2018 [accessed]. https://www.us-cert.gov/ccubedvp/self-service-crr

[WH 2013a]
Executive Order – Critical Infrastructure Security and Resilience. *The White House.* 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[WH 2013b]
Executive Order – Improving Critical Infrastructure Cybersecurity. *The White House*. 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY
   (Leave Blank)

2. REPORT DATE
   March 2018

3. REPORT TYPE AND DATES COVERED
   Final

4. TITLE AND SUBTITLE
   A Mapping of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the Cyber Resilience Review (CRR)

5. FUNDING NUMBERS
   FA8721-05-C-0003

6. AUTHOR(S)
   Greg Porter, Matt Trevors, Robert A. Vrtis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
   Software Engineering Institute
   Carnegie Mellon University
   Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
   CMU/SEI-2018-TN-001

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
   AFLCMC/PZE/Hanscom
   Enterprise Acquisition Division
   20 Schilling Circle
   Building 1305
   Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
    n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
    Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

This technical note provides a description of the methodology used and observations made while mapping the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the practice questions found in the CERT® Cyber Resilience Review (CRR). The mapping allows health care and public health organizations to use CRR results not only to gauge their cyber resilience, but to examine their current baseline with respect to the HIPAA Security Rule and the NIST Cybersecurity Framework (CSF). The CRR and HIPAA Security Rule has been mapped to the NIST CSF. The authors used these mappings and their extensive experience with CRRs to propose the mapping found in this technical note. The mappings between the CRR practices and the HIPAA Security Rule are intended to be informative and do not imply or guarantee compliance with any laws or regulations. The proposed mapping shows that the CRR provides complete coverage of the HIPAA Security Rule. As a result, organizations that must adhere to the HIPAA Security Rule can use the CRR to indicate their compliance with the Security Rule.

14. SUBJECT TERMS
    Health Insurance Portability and Accountability Act Security Rule, HIPAA, Cyber Resilience Review, CRR, CRR Crosswalk, mapping

15. NUMBER OF PAGES
    55

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
    Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
    Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
    Unclassified

20. LIMITATION OF ABSTRACT
    UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102